Opening Statement - Ranking Member Cedric L. Richmond

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

"Industry Perspectives on the President's Cybersecurity Information Sharing Proposal"

March 4, 2015, 2 p.m.

Our infrastructure is more digitally interconnected than ever. Our country's reliance on cyber systems and networks covers everything from power plants to pipelines, and hospitals to highways. Yet for all the advantages interconnectivity offers, our nation's critical infrastructure is also increasingly vulnerable to attack from an array of cyber threats.

We are to hear testimony today on how we can be better prepared for these threats. The President has proposed an updated package of legislative initiatives to frame the issues, and hopefully spur Congress to action on cybersecurity. Last year this Subcommittee was the author of important authorizations that gave the Department sound footing to carry out its mission as the central civilian portal for information-sharing between critical infrastructure sectors and the government.

It is widely recognized that more is needed, and the President's initiatives do indeed go further. Senator Carper, Ranking Member on the Senate Homeland Security and Government Affairs Committee, has already introduced almost a word for word version of the White House information-sharing language as S. 456, *The Cyber Threat Sharing Act of 2015.*

Hacks on major businesses and financial institutions continue to dominate headlines. Just a few weeks after Anthem insurance announced that account information of as many as 80 million customers had been stolen, we are all waiting for the next shoe to fall.

The President's proposal seeks to create a friendlier atmosphere for companies to swap certain types of computer data with each other and the government, in order to identify potential cyber threats and isolate security flaws. To persuade companies to buy into the proposed system, the White House bill would provide assurances that the sharing of indicators—which could include things like IP addresses, routing information, and date and time stamps deemed important to identifying potential cyber threats or security vulnerabilities—would be exempt from legal or regulatory punishment. The President's proposals contain some new ideas about the formation of information-sharing organizations that would set sharing standards and privacy requirements.

Since the '90s, firms have shared information directly on an ad hoc basis and through private sector, nonprofit organizations, such as Information Sharing and Analysis Centers, or ISACs that can analyze and disseminate information. The White House proposal requires the Secretary of Homeland Security to form a new type of organization, the *Information Sharing and Analysis Organizations*, or ISAOs.

We need to know what kinds of barriers to information-sharing exist today, and how we on this Subcommittee can help make this cyber tool more effective. For our side, information-sharing must be structured in the public and private sectors to ensure that the risks to privacy rights and civil liberties of individual citizens be recognized, and how those rights and liberties can best be protected. Today, hopefully we'll find answers to some of these questions.

We live in a post-Snowden world, and we are all much more aware of the powerful abilities of our surveillance agencies. Information-sharing is not a zero-sum game. As policy makers we can step back and take stock of how best to protect our citizen's privacy rights, while finding effective and powerful tools to combat the cyber threats before us.